UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/720,085	12/20/2000	Louis Goubin	T2146-906752	6949

181 7590 05/19/2005

MILES & STOCKBRIDGE PC
1751 PINNACLE DRIVE
SUITE 500
MCLEAN, VA 22102-3833

EXAMINER	
SON, LINH L D	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 05/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/720,085	GOUBIN ET AL.	
	Examiner	Art Unit	
	Linh LD Son	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 December 2000*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *14-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *14-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This written action is responding to the amendment received on January 07th, 2005.

2. Claims 14-34 are amended. Claims 1-13 are canceled.

3. Claims 14-34 are pending

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 14-34 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The language of the claim raises a question as to whether the claim is directed merely to an abstract idea that is not tied to a technological art, environment or machine which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. 101. Claims 14-34 consist solely of mathematical operations without practical application in the technological arts or simply manipulate abstract ideas without practical application in the technological arts.

6. To expedite a complete examination of the instant application the claims rejected under 35 U.S.C. 101 (Non-statutory) above are further rejected as set forth below in anticipation of applicant amending these claims to place them within the four statutory categories of invention.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 14 are rejected under 35 U.S.C. 102(e) as being anticipated by Ebihara et al, hereinafter "Ebihara", US Patent No. 5982900.

9. As per claim 14, Ebihara discloses the "Circuit and System for Modulo Exponentiation Arithmetic and Arithmetic Method of Performing Modulo Exponentiation Arithmetic" invention, which teaches a method for verifying a signature, or respectively an authentication, utilizing an asymmetric private-key and public-key (Col 1 lines 29-34) cryptographic calculation process between a

prover entity (Person A) and a verifier entity (Person B), wherein the prover entity performs first cryptographic calculations with said private key to produce a signature calculation (Col 2 lines 50-63), or respectively an authentication value (Signature) constituting a response value , and the verifier entity, based on said response value, performs second cryptographic calculations with said public key to perform said signature verification, or respectively said authentication (Col 2 line 63 to 67), the first and second cryptographic calculations serving to implement the calculation of modulo-n or large number multiplications (Col 2 line 50 to Col 5 line 35), characterized in that for a cryptographic calculation process using a public key comprising a public exponent e and a public modulo n (Col 2 lines 53-62 and Col 4 lines 45-67), and a private key comprising a private exponent (Col 2 line 65 to Col 3 line 5), it comprises the following steps: calculating at the level of said prover entity at least one pre-validation value (CA, Col 2 line 56); transmitting from the prover entity to the verifier entity at least said one pre-validation value (Col 3 line 8), and utilizing said pre-validation value by the verifier entity to perform at least one modular reduction without any division operation for said modular reduction (Col 3 lines 1-42, and Col 5 lines 43-60). Montgomery's reduction is an arithmetic reduction performing without any division operation (Col 7 lines 30-50).

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 15-18, 21-27, and 31-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ebihara in view of Menezes, Blind Signature Schemes, Chapter 11.8.1 Pg 475.

12. As per claim 15, Ebihara teaches "**a method according to claim 14, wherein the cryptographic calculation process is based on a Rabin Algorithm**" in (Col 1 lines 35-49). Rabin Algorithm is an improvement of RSA, which is used to verify and authenticate a signature. As explained in Column 2 from lines 6-28, and lines 50-67, Party A wants to authenticate to Party B by calculating a signature encrypted using the secrete key. $CA=M^d$ modn signature, then get transmit over to Party B for verification. However, Ebihara does not teach the Quotient $Q=R^k/n$ or $Q=CA^k/n$ where CA=R= signature and k is any integer. Nevertheless, the Quotient is a method of blinding the signature before sending it to the verifier. Instead of sending the signature to the verifier, the signature gets blinded by a process of k exponent and divides by an n factor. Since both the verifier and the prover know the n value, the signature can be easily recovered by a simple multiplication of n. It is common to use the blinding

signature method in the art to prevent ease-drop attack (See Blind Signature on Page 475). Therefore, it would have been obvious for one having ordinary skill in the art at the time of the invention was made to incorporate the blind signature method to calculate the pre-validation value before sending it to the partner. In addition, the blind signature method would not be a burden on the smart card side, since the heavy calculation processing has already been done on the card reader side.

13. As per claim 16, the blinding signature method is incorporated. Further, the RSA signature verification method is also included to verify the message authenticity taught in (Ebihara, Col 2 lines 6-28). Based on the RSA signature verification algorithm, the verification is concluded when both the sent signature and the decrypted signatures are equal or the difference is zero. The $(D_{AR}, D_{SR}) = R*R = Q*n$ equation does just that.

14. As per claim 17, Claim 15 is incorporated. However, the Quotient Q2 is not directly taught. Nevertheless, Q2 equation is formulated to R*(R*R-Q1*n)/n so that the result of the signature verification is equal to Zero. This verification method is common in art and also taught by the RSA (See Ebihara Col 2 lines 6-28). The verification process is concluded when the decrypted message is the same as the sent message or another word the difference of the messages equals to zero. In additional, the blind signature method is also implemented in the formulation of Q_2 (See Claim 15 basis of rejection using the blind

Signature), where the equation is divided by n. Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to incorporate the blind signature and the RSA signature verification method into Ebihara's invention to reduce the processing burden on the Smart card processor which is limited.

15. As per claim 18, the blinding signature and the RSA signature verification method described in claims 15, 16 and 17 are also applied.

16. As per claims 21 and 22, "**A method according to claims 16 and 18, characterized in that, for an authentication verification operation, said method further comprises the step for transmitting a prompt value from the verifier entity to the prover entity**" is taught by Ebihara in (Col 2 lines 6-28). The prompt value in Col 2 lines 6-28 is the message M, which is not limited to the text message. The message must be originated from party B in order to verify the received message is the same as the original.

17. As per claims 23 and 24, "**A method according to claims 21 and 22, characterized in that said prompt value comprises a random value A modulo n, said response value R comprises an encrypted value B, and said function of the response value comprises a function f(A) of said**

random value A" is taught by Ebihara in (Col 2 lines 6-28). As rejected in claims 21 and 22, the f(A) is recited as $f(M) = M^d \bmod n$.

18. As per claims 25-27, "**A method according to claims 16 and 21-22, characterized in that said function f(A) if said random value A comprises a function among the functions f(A)=A**" is taught by Ebihara in (Col 2 lines 6-28). The function taught is M^d modn. If n = 1 and d=1, then f(A) = A. However, the "f(A)=n-A, f(A)= C*Amodn, f(A)= -C*A modn" is not taught by Ebihara. Nevertheless, the result of the f(A) is depending on a mathematical functions f (A mod n). Therefore it would have been obvious at the time of the invention was made for one having ordinary skill in the art to implement plurality of different mathematical functions to acquire different results to add more verification steps of the signature.

19. As per claims 31 and 32, "**A method according to claim 23, characterized in that said function f(A) of said random value A is the function f(A)=A, which makes it possible to verify the equality of said difference and the validity of said authentication without any division operation for the modular reduction**" is taught by Ebihara in (Col 3 lines 1-42, and Col 5 lines 43-60). Montgomery's reduction is an arithmetic reduction performing without any division operation (Col 7 lines 30-50).

20. Claims 28-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ebihara in view of Menezes, and further in view of Stinson, Cryptography theory and Practice, CRC Press, Inc. page 3, hereinafter "Stinson".

21. As per claims 28, 29, and 30, Ebihara and Menezes do not clearly teach "**a method according to claim 25, 26, and 27, characterized in that at the level of the verifier entity, the calculation of said function f(A)=C*A mod n comprises calculation of the value C*A and storing of said value if C*A < n, and the calculation and storing of the value C*A – n if not, and in that calculation of said function f(A) = -C*A modulo n comprises calculation of the value n-C*A and storing of said value if n-C*A ≥ 0, and otherwise calculation of the intermediate value C*n-C*A, and if said intermediate value is greater than or equal to zero, calculation and storing of the value of –C*A modulo n, for verifying the equality of said authentication without any division for the modular reduction**". Nevertheless, the modular reduction method in the claim is the basic mathematic of modular reduction comprise of multiplication and subtraction only. The same method is explained in Stinson on page 3, (the definition 1.2). The C is similar to q1 and r1 is the remainder of a division of m by b. The checking of the difference less than or equal to 0 is to find out the arithmetic completed or not. Therefore, it would have been obvious at the time of the invention was made for one having

ordinary skill in the art to implement the modular reduction method without any division by trying number of variables until the remainder is found. The method would require minimal processing capacity given that n is not sufficiently large.

22. **Claims 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ebihara in view of Menezes, and further in view of Poore et al, US Patent No. 6202933B1, hereinafter "Poore".**

23. As per claims 19 and 20, "**the applying a condensation function to said message to obtain a message digest CM; and concatenating said message digest with a constant value** " is not taught by Ebihara and Menezes. Nevertheless, the feature is taught clearly by Poore in (Col 4 lines 52-56). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify the invention to include Poore's teaching so that the signature is further be verified by using its digest.

24. **Claim 33 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ebihara in view of Poore et al, US Patent No. 6202933B1, hereinafter "Poore".**

25. As per claim 33, claims 14, 15, and 17 are incorporated to reject the encrypted value B, and a quotient value Q. However, Ebihara does not teach the

concatenation of the two values. Nevertheless, it is taught in Poore in (Col 4 lines 52-56). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to combine Poore's teaching to add a security feature to the message transferring process.

26. **Claim 34 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ebihara in view of Liskov et al, US Patent No. 6411715B1, hereinafter Liskov.**

27. As per claim 34, a method according to claim 14, "**wherein the verifier entity compression embedded system such as a microprocessor card and the prover entity comprises an embedded card reading system**" is not taught by Ebihara. Nevetheless, Liskov teaches a method and apparatus for verifying the cryptographic security keys where the authentication process is utilized in microprocessor card and a card reading apparatus (Col 7 lines 5-15, Col 6 lines 50-65). Therefore, it would have been obvious at the time of the invention was made for one of ordinary skill in the art to incorporate Ebihara's teaching in the smart card technology to reduce the processing power and time which is limited in the technology.

Response to Amendment

28. As per Amendment made to overcome 35 U.S.C. 101 rejection has been fully considered but they are not persuasive. Applicant amended:

29. Claim 14. (Currently Amended) A method for verifying a signature, or respectively an authentication, utilizing an asymmetric private-key and public-key cryptographic calculation process between a "prover" entity and a "verifier" entity, **said prover entity including communication means for communicating with said verifier entity** wherein the prover entity performs first cryptographic calculations with said private key to produce a signature calculation, or respectively an authentication value constituting a response value, and the verifier entity, based on said response value, performs second cryptographic calculations with said public key to perform said signature verification, or respectively said authentication, the first and second cryptographic calculations serving to implement the calculation of modulo-n or large-number multiplications, wherein for a cryptographic calculation process using a public key comprising a public exponent e and a public modulo n, and a private key comprising a private exponent, said method further comprises: calculating at the level of said prover entity at least one prevalidation value; **using the communication means of the prover entity for** transmitting to the verifier entity, in addition to said signature calculation or response value, at

least said one prevalidation value, and utilizing said prevalidation value by the verifier entity to perform at least one modular reduction without any division operation for said modular reduction.

30. The communication means amended does not provide enough support to practical application in the technological arts. The communication means can be interpreted as hand delivery of a written math calculation between two persons where one is a prover and the other is the verifier. Therefore, 35 U.S.C. 101 rejection is maintained.

Response to Arguments

31. Applicant's arguments filed 01/07/05 have been fully considered but they are not persuasive.

32. As per argument on page 8 3rd paragraph, Applicant argued that Ebihara fail to teach or suggest the prevalidation value and utilizing said prevalidation value by the verifier entity to perform at least one modular reduction without any division operation. As examiner cited, the pre-validation value is CA (Col 2 line 56), which is encrypted and sent to the Verifier to perform calculation. It is showed clearly that CA is the pre-validation value since it is a value used to verify the identity of Party A to Party B. The calculation steps for verification in Col 3 can also be done by Montgomery reduction, which is shown in (Col 7 lines 30-40, Col 7 line 50 to Col 10 line 45) to carry out the classical modular

reduction by multiplication (See also Handbook of Applied cryptography, by Alfred J. Meneze, dated 1997, page 600-601). Therefore, Claims 14-34 rejection dated 09/08/04 is maintained.

Conclusion

33. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

34. Any inquiry concerning this communication from the examiner should be directed to Linh Son whose telephone number is (571)-272-3856.

35. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor Kim Y. Vu can be reached at (571)-272-3859. The fax numbers for this group are (703)-872-9306 (official fax). Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the group receptionist whose telephone number is (571)-272-2100.

36. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval IPAIR.I system. Status information for published applications may be obtained from either Private PMR or Public PMR. Status information for unpublished applications is available through Private PMR only. For more information about the PAIR system, see http://pzr-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AU 2135

Linh LD Son

Patent Examiner